

On the quasi group of a cubic surface over a finite field

Andreas-Stephan Elsenhans* and Jörg Jahnel[‡]

Abstract

We construct nontrivial homomorphisms from the quasi group of some cubic surfaces over \mathbb{F}_p into a group. We show experimentally that the homomorphisms constructed are the only possible ones and that there are no nontrivial homomorphisms in the other cases. Thereby, we follow the classification of cubic surfaces, due to A. Cayley.

1 The quasi group of a cubic surface

1.1. — According to Yu.I. Manin [Ma], a cubic surface V carries a structure of a *quasi group*. For us, this shall simply mean the ternary relation

$$[x_1, x_2, x_3] \iff x_1, x_2, x_3 \text{ non-singular, intersection of } V \text{ with a line.}$$

If V is defined over a field K then, on $V^{\text{reg}}(K)$, there is a structure of a quasi group.

1.2. — Here, the precise definition is that the lines lying entirely on the surface shall *not* cause any relation. On the other hand, it is allowed that two or all three points coincide. Then, the line shall simply be tangent to the surface of order two or three.

1.3. Definition. — Let $(\Gamma, [])$ be a quasi group and $(G, +)$ be an abelian group. By a homomorphism $p: \Gamma \rightarrow G$, we mean a mapping such that, for a suitable $g \in G$,

$$p(x_1) + p(x_2) + p(x_3) = g$$

*Mathematisches Institut, Universität Bayreuth, Univ'straße 30, D-95440 Bayreuth, Germany, Stephan.Elsenhans@uni-bayreuth.de, Website: <http://www.staff.uni-bayreuth.de/~btm216>

[‡]Fachbereich 6 Mathematik, Universität Siegen, Walter-Flex-Str. 3, D-57068 Siegen, Germany, jahnel@mathematik.uni-siegen.de, Website: <http://www.uni-math.gwdg.de/jahnel>

*The first author was supported in part by the Deutsche Forschungsgemeinschaft (DFG) through a funded research project.

[‡]Key words: Cubic surface, Cayley's classification, quasi group, Mordell-Weil group, Suslin's homology. MSC: 14J26, 14J20, 14G15, 11G25

whenever $[x_1, x_2, x_3]$ is true.

1.4. Fact. — The category of all homomorphisms from a quasi group Γ to abelian groups has an initial object. The corresponding abelian group is $\underline{\Gamma} := \mathbb{Z}\Gamma/N$, for N the subgroup generated by $1 \cdot x_1 + 1 \cdot x_2 + 1 \cdot x_3 - 1 \cdot x'_1 - 1 \cdot x'_2 - 1 \cdot x'_3$ for all $[x_1, x_2, x_3]$ and $[x'_1, x'_2, x'_3]$.

$\underline{\Gamma}$ carries a surjective augmentation homomorphism $s: \underline{\Gamma} \rightarrow \mathbb{Z}$. We will call $\ker s$ the group associated with Γ .

1.5. Definitions. — Let V be a cubic surface over a field K .

i) We will call the group associated with the quasi group $V^{\text{reg}}(K)$ the *Mordell-Weil group* of V . It will be denoted by $\text{MW}(V)$.

ii) We will call two points $x_1, x_2 \in V^{\text{reg}}(K)$ *equivalent* if $[x_1] - [x_2] = 0 \in \text{MW}(V)$.

1.6. Example. — Let V be the *Cayley cubic* given by the equation

$$xyz + xyw + xzw + yzw = 0$$

in \mathbf{P}^3 over a field K . Then, for a non-singular point $p = (x_0 : y_0 : z_0 : w_0) \in V(K)$, either no coordinate vanishes or exactly two of them. Accordingly, put

$$s(p) := \begin{cases} x_0 y_0 z_0 w_0 & \text{if } x_0, y_0, z_0, w_0 \neq 0, \\ - \prod_{v=x_0, y_0, z_0, w_0 \neq 0} v & \text{otherwise.} \end{cases}$$

Further, let l be a line in \mathbf{P}^3 not contained in V and denote by p_1, p_2 , and p_3 the intersection points with V , which are supposed to be non-singular and K -rational and counted with multiplicity.

Then, $s(p_1)s(p_2)s(p_3)$ is a perfect square in K .

Proof. This observation is easily checked by calculations in `maple`, treating the possible cases separately. \square

1.7. Example (continued). — For V the Cayley cubic over K , the map s therefore induces a surjective homomorphism of groups

$$\text{MW}(V) \longrightarrow K^*/(K^*)^2.$$

i) In particular, for the Cayley cubic over \mathbb{Q} , the group $\text{MW}(V)$ is not finitely generated.

ii) On the other hand, for the Cayley cubic over a finite field \mathbb{F}_q of odd characteristic, we have $\text{MW}(V) \cong \mathbb{Z}/2\mathbb{Z}$. There are two different kinds of smooth points on V . Two points $p_1, p_2 \in V^{\text{reg}}(\mathbb{F}_q)$ are equivalent if and only if $s(p_1)s(p_2)$ is a square.

The purpose of this article is to investigate this phenomenon more systematically.

1.8. Remark. — The Mordell-Weil group is related to the famous *Mordell-Weil problem*, which may be formulated as to find a minimal system of generators for $\text{MW}(V)$.

1.9. — We are particularly interested in the cases when, for V a cubic surface over a finite field, $\text{MW}(V) \neq 0$. The point is that there is the following

Application. Let \mathcal{V} be a cubic surface over \mathbb{Q} and p_1, \dots, p_t be primes satisfying the following conditions.

- i) There is no \mathbb{F}_{p_i} -rational line contained in the reduction \mathcal{V}_{p_i} .
- ii) The singularities of \mathcal{V}_{p_i} do not lift to smooth \mathbb{Q} -rational points on \mathcal{V} .

Then, the reductions induce a natural homomorphism

$$\text{MW}(\mathcal{V}) \longrightarrow \text{MW}(\mathcal{V}_{p_1}) \times \dots \times \text{MW}(\mathcal{V}_{p_t}).$$

If \mathcal{V} has weak approximation then this map is a surjection.

1.10. — There is another application, which is related to the so-called Brauer-Manin obstruction. This is a method, invented by Yu. I. Manin [Ma, Chapter. VI], to explain the failure of the Hasse principle or weak approximation in certain cases. It is based on the consideration of a non-trivial Brauer class $\alpha \in \text{Br}(\mathcal{V})$ and the corresponding p -adic evaluation maps

$$\text{ev}_{\alpha,p}: \mathcal{V}(\mathbb{Q}_p) \longrightarrow \text{Br}(\mathbb{Q}_p) = \mathbb{Q}/\mathbb{Z}, \quad x \mapsto \alpha|_x.$$

Proposition. Let $p \neq 2$ be a prime number and $F \in \mathbb{Z}_p[X_0, X_1, X_2, X_3]$ cubic form defining a smooth cubic surface \mathcal{V} over \mathbb{Q}_p . Suppose that all $x \in \mathcal{V}(\mathbb{Q}_p)$ specialize to $\mathcal{V}_p^{\text{reg}}$ and that $\text{MW}(\mathcal{V}_p) = 0$.

Then, $\text{ev}_{\alpha,p}$ is constant for every $\alpha \in \text{Br}(\mathcal{V})$.

Proof. It is known that $\text{ev}_{\alpha,p}(x)$ depends only on the reduction of x modulo p [B, Theorem 1]. Further, an application of Lichtenbaum duality [Li, Corollary 1] proves that $\text{ev}_{\alpha,p}$ is induced by a group homomorphism $\text{MW}(\mathcal{V}_p) \rightarrow \mathbb{Q}/\mathbb{Z}$. \square

1.11. Remark. — In [EJ], we studied explicit examples of cubic surfaces, for which the Brauer-Manin obstruction works at certain primes. It was noticeable in the experiments that the reduction types at the relevant primes were distributed in an unusual way. Reducible reductions and reductions to the Cayley cubic occurred frequently. This observation was actually the starting point of our investigations on the Mordell-Weil group.

1.12. — The goal of this article is to compare $\text{MW}(V)$ with a group more tractable from the theoretical point of view. For cubic surfaces that are not

too degenerate, this will be $A_0(V^{\text{reg}})$, the degree-0 part of Suslin's homology group $h_0(V^{\text{reg}})$. We will establish a canonical homomorphism

$$\pi_V: \text{MW}(V) \longrightarrow A_0(V^{\text{reg}})$$

for V a geometrically irreducible cubic surface over a finite field. Under minimal assumptions, π_V will be surjective.

1.13. Plan of the article. — In section 2, we will recall Cayley's classification of cubic surfaces. After this, we will consider two degenerate cases at first. Section 3 will be concerned with the situation of a cone. Then, there is a surjection to the Mordell-Weil group of the underlying curve. Section 4 will treat the reducible case. It will turn out that there is a nontrivial surjection from $\text{MW}(V)$ to a nontrivial abelian group, which is given in an elementary manner. In section 5, we will construct the homomorphism π_V . Then, we will compute $A_0(V^{\text{reg}})$ systematically for each of the remaining cases of the classification of cubic surfaces.

At the end of the main body of the article, we will report on the comparison between $\text{MW}(V)$ and $A_0(V^{\text{reg}})$ in a large sample of examples. In an appendix, we will discuss efficient algorithms to compute $\text{MW}(V)$ for a concrete surface.

2 Cayley's classification of cubic surfaces

2.1. — Cubic surfaces are classified since the days of A. Cayley [Do, sec.9.2]. According to this, there are the following types.

I) A normal cubic surface is either

i) in one of the 21 classes of surfaces with finitely many double points, listed in [Do, Table 9.2.5]. This includes the case of a smooth cubic surface.

ii) Or the cone over a smooth cubic curve C .

II) A non-normal, geometrically irreducible cubic surface is either

i) a cubic ruled surface. There are two types of those [Do, Theorem 9.2.1], ordinary and Cayley's cubic ruled surfaces.

ii) Or the cone over a singular cubic curve. This might be a cubic with a self-intersection or a cusp.

2.2. — In the situation of a finite base field, the classification of geometrically irreducible cubic surfaces is actually a little finer.

I.i) Among these types, $2A_1$, $3A_1$, $2A_2$, $A_2 + 2A_1$, $4A_1$, $2A_2 + A_1$, $A_3 + 2A_1$, and $3A_2$ have symmetries. This leads to 13 further types, where the singularities are defined over extensions of the ground field.

II.i) An ordinary cubic ruled surface may have its normal form $xz^2 + yw^2 = 0$ only over a quadratic extension. This causes a third type of cubic ruled surfaces over a finite field.

II.ii) In the case of the cone over a cubic curve with self-intersection, there are two variants as to whether the two tangent directions at the point of intersection are defined over the ground field or not.

2.3. — We will restrict ourselves to reduced cubic surfaces. In other words, the following types of reducible surfaces are allowed.

i) A reducible cubic surface might consist of a quadric and a plane. There are four cases where the quadric is nondegenerate. In fact, the quadric may split over the ground field or not and the plane may be tangent or not. There are four more cases when the quadric is a cone. The intersection with the plane might be a conic, two lines, a double line, or a point.

ii) Finally, the surface might be reducible into three planes. There are two cases as to whether their intersection is a point or a line. Observe that it is possible that the decomposition into three planes is defined only after a finite field extension.

3 The case of a curve

3.1. — Let $C \subset \mathbf{P}^2$ be a reduced cubic curve over a field K . Then, in a manner analogous to the surface case, there are a quasi group structure on C and the *Mordell-Weil group* $\text{MW}(C)$. This group is known in every case.

i) It may happen that all K -rational smooth points are contained in a line. Then, the quasi group structure is empty and $\text{MW}(C) = \ker(\text{sum}: \mathbb{Z}[L(K)] \rightarrow \mathbb{Z})$. We have this degenerate case whenever C contains a line defined over a proper extension of K . The same may happen even for a smooth cubic curve when $\#K \leq 5$. Otherwise,

ii) $\text{MW}(C) = J(C)(K)$ for C smooth, and

iii) $\text{MW}(C) = K^+$ if C is a cubic curve with a cusp.

iv) If C is a cubic curve with a node then $\text{MW}(C) = K^*$ in case that the two tangent directions at the node are defined over K . If the tangent directions are defined over the quadratic extension F/K then $\text{MW}(C) = \ker(N: F^* \rightarrow K^*)$.

v) When C is reducible into a line and a conic then $\text{MW}(C) = \ker(N: F^* \rightarrow K^*) \oplus \mathbb{Z}$, $\text{MW}(C) = K^+ \oplus \mathbb{Z}$ or $\text{MW}(C) = K^* \oplus \mathbb{Z}$ depending on whether, over K , there are no, one, or two points of intersection.

vi) When C is reducible into three components then $\text{MW}(C) = K^+ \oplus \mathbb{Z}^2$ or $\text{MW}(C) = K^* \oplus \mathbb{Z}^2$ depending on whether the three points of intersection coincide or not. In the case of three points of intersection, this is actually Menelaos' Theorem.

3.2. Fact (Cones). — For V a cone over a cubic curve C , we have a canonical surjection $\text{MW}(V) \rightarrow \text{MW}(C)$.

4 Reducible cubic surfaces

4.1. — Let V be a reducible cubic surface over a field K . Then, there are two essentially different cases.

i) There are two irreducible components, a plane E and a quadric, but the quadric consists of two planes defined over a quadratic extension. Then, only the plane E contains K -rational smooth points. We have an empty quasi group structure and $\text{MW}(V) = \ker(\text{sum}: \mathbb{Z}[E(K)] \rightarrow \mathbb{Z})$.

ii) Otherwise, when V decomposes into $k = 2, 3$ components, there is a canonical surjection $\text{MW}(V) \twoheadrightarrow \ker(\text{sum}: \mathbb{Z}^k \rightarrow \mathbb{Z}) \cong \mathbb{Z}^{k-1}$.

4.2. Example. — Over a finite field \mathbb{F}_q of characteristic $\neq 2$, let V be a reducible cubic surface consisting of a nondegenerate quadratic cone Q and a plane E . Suppose that E does not meet the cusp of Q . Then, there is a canonical surjection

$$\text{MW}(V) \twoheadrightarrow \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}.$$

Proof. The homomorphism to \mathbb{Z} is that from 4.1.ii). It remains to construct the homomorphism to $\mathbb{Z}/2\mathbb{Z}$.

For this, we fix coordinates such that the cusp is in $(1 : 0 : 0 : 0)$ and the plane E is given by $x = 0$. Further, we assume without restriction that the plane “ $y = 0$ ” is tangent to the cone Q . Then, the cone is given by, say, $yz + Kw^2 = 0$ for $K \neq 0$. The whole cubic surface has the equation

$$x(yz + Kw^2) = 0.$$

On the plane “ $x = 0$ ”, we define the homomorphism $\text{MW}(V) \rightarrow \mathbb{Z}/2\mathbb{Z}$ simply as $\chi_2(K(yz + Kw^2))$ for χ_2 the quadratic character on \mathbb{F}_q^* . On the cone “ $yz + Kw^2 = 0$ ”, we take $\chi_2(xy)$, respectively $\chi_2(-Kxz)$ when $y = 0$.

We have to show that this definition is indeed compatible with the quasi group structure. For this, let $(x : y : z : w) \in Q(\mathbb{F}_q)$, $(x' : y' : z' : w') \in Q(\mathbb{F}_q)$, and $(0 : y'' : z'' : w'') \in E(\mathbb{F}_q)$ be three collinear points. Then, we clearly have $(0 : y'' : z'' : w'') = (0 : (x'y - xy') : (x'z - xz') : (x'w - xw'))$. Furthermore,

$$\begin{aligned} (xy)(x'y')K(y''z'' + Kw''^2) &= Kxx'y'y'[(x'y - xy')(x'z - xz') + K(x'w - xw')^2] \\ &= -Kxx'y'y'[xx'(yz' + y'z + 2Kww')] \\ &= -Kx^2x'^2(-Ky^2w'^2 - Ky'^2w^2 + 2Kyy'ww') \\ &= K^2x^2x'^2(yw' - y'w)^2 \end{aligned}$$

is a perfect square. □

5 Irreducible cubic surfaces not being cones

5.0.1. — When a cubic surface V is irreducible, but geometrically reducible, then it consists of three planes acted upon transitively by the Galois group. In this case, $V^{\text{reg}}(K) = \emptyset$ and, therefore, $\text{MW}(V) = 0$. Thus, we may restrict ourselves to the geometrically irreducible case.

5.1 Suslin's singular homology group h_0

5.1.1. — For a scheme of finite type over a field K , the singular homology groups $h_*(S)$ were introduced by A. Suslin [SV]. We will only need $h_0(S)$, for which there is the following elementary description.

5.1.2. Fact. — *Let S be an integral scheme of finite type over a field K . Then,*

$$h_0(S) = Z_0(S) / \text{Rat}'_0(S).$$

Here, $Z_0(S)$ is the group of 0-cycles, i.e., the free abelian group over all closed points of S . $\text{Rat}'_0(S)$ is generated by all 0-cycles of the following kind.

Let $C \subset S$ be an irreducible curve, C' its normalization, and \overline{C} the corresponding smooth, proper model. Then, take all the cycles $\text{div}(f)$ where $f \not\equiv 0$ is a rational function on C which, after pull-back to \overline{C} , is constantly 1 on $\overline{C} \setminus C'$.

Proof. See [Sch, Theorem 5.1]. □

5.1.3. Remarks. — a) $h_0(S)$ is equipped with a natural map $\text{deg}: h_0(S) \rightarrow \mathbb{Z}$. We will denote its kernel by $A_0(S)$.

b) Let $i: S_1 \rightarrow S_2$ be an arbitrary morphism of quasi-projective varieties over K . Then, there is the induced homomorphism $i_*: h_0(S_1) \rightarrow h_0(S_2)$, $[x] \mapsto [i(x)]$. This immediately yields a map $i_*: A_0(S_1) \rightarrow A_0(S_2)$.

5.1.4. Lemma. — *Let V be a geometrically irreducible cubic surface over \mathbb{F}_q . Then, there is a canonical homomorphism*

$$\pi_V: \text{MW}(V) \rightarrow A_0(V^{\text{reg}}).$$

Proof. To each combination $a_1[p_1] + \dots + a_k[p_k]$ for $p_1, \dots, p_k \in V^{\text{reg}}(K)$ and $a_1 + \dots + a_k = 0$, the homomorphism i_* assigns the corresponding cycle. We take this as a definition for π_V . To show that π_V is well-defined, we have to verify the following.

Assume that x_1, x_2, x_3 are collinear and x'_1, x'_2, x'_3 are collinear, too. Suppose that the connecting lines are not contained in V . Then,

$$[x_1] + [x_2] + [x_3] - [x'_1] - [x'_2] - [x'_3] = 0 \in A_0(V^{\text{reg}}).$$

For this, consider the pencil of planes through x_1, x_2, x_3 . Generically, the intersection with V is a curve, smooth at x_1, x_2 and x_3 . The only possible exceptions are the tangent planes. We claim that the generic intersection curve is irreducible, too. Indeed, the contrary would mean that all intersection curves contained a line. Suppose, this is a line through x_1 . Then, V contains a pencil of lines through x_1 , which implies V contains a plane through x_1 . Hence, V is reducible, a contradiction.

Thus, take a plane through x_1, x_2, x_3 , generating an irreducible intersection curve C that is smooth in x_1, x_2 and x_3 . Further, take a plane through x'_1, x'_2, x'_3 generating an irreducible intersection curve C' that is smooth in x'_1, x'_2 and x'_3 and meets C only in smooth points x''_1, x''_2, x''_3 . The sublemma below, applied to C and C' , immediately yields the assertion. \square

5.1.5. Sublemma. — *Let C be an irreducible cubic curve. Assume that $p_1, p_2, p_3 \in C^{\text{reg}}$ as well as $q_1, q_2, q_3 \in C^{\text{reg}}$ are triples of collinear points such that $\{p_1, p_2, p_3\} \cap \{q_1, q_2, q_3\} = \emptyset$.*

Then, there is a rational function f on C having simple zeroes at p_1, p_2, p_3 , simple poles at q_1, q_2, q_3 , no other zeroes or poles, and the value 1 at the possible singular point.

Proof. According to J. Plücker, an irreducible cubic curve may have at most one singular point. We may therefore put $f := K \cdot l_1/l_2$ for forms l_1 and l_2 defining the lines. By assumption, these do not meet the singular point. If necessary, we choose the constant K such that the value at the singularity is normalized to 1. \square

5.2 h_0 and the tame fundamental group

5.2.1. — Let S be a smooth surface over the finite field \mathbb{F}_q for $q = p^r$ and let $\overline{S} \supseteq S$ be a smooth compactification. Then, the *tame fundamental group* $\pi_1^t(S)$ of S classifies all finite coverings of S which are tamely ramified at $\overline{S} \setminus S$.

The group $\pi_1^t(S)$ is independent of the choice of the compactification \overline{S} . $\pi_1^t(S)$ is a quotient of $\pi_1^{\text{ét}}(S)$. By the purity of the branch locus [SGA1, Exp. X, Théorème 3.1], one has

$$\pi_1^t(S)_{\text{tors}}^{\text{ab}} \cong (\pi_1^{\text{ét}}(S)^{\text{ab}})_{\text{prime to } p} \oplus (\pi_1^{\text{ét}}(\overline{S})^{\text{ab}})_{p\text{-power}}.$$

Again, this decomposition is independent of the choice of \overline{S} .

The structural morphism $S \rightarrow \text{Spec } \mathbb{F}_q$ induces a surjection $\pi_1^t(S) \rightarrow \pi_1(\text{Spec } \mathbb{F}_q)$ the kernel of which we will denote by $\pi_1^{t, \text{geo}}(S)$. Note that $\pi_1^{t, \text{geo}}(S)$ differs from $\pi_1^t(S_{\overline{\mathbb{F}}_q})$. The point is that the analogue of the natural short exact sequence [SGA1, Exp. IX, Théorème 6.1] is only right exact for the tame fundamental group.

5.2.2. Theorem (Schmidt, Spieß). — *Let S be a surface over a finite field \mathbb{F}_q which is smooth and geometrically irreducible, but not necessarily proper.*

i) *Then, $A_0(S)$ is a finite abelian group.*

ii) *There is a canonical isomorphism $\iota_S: A_0(S) \longrightarrow \pi_1^{t,\text{geo}}(S)^{\text{ab}}$.*

Proof. See [SchS, Theorem 0.1]. □

5.2.3. Remarks. — a) Concretely, ι_S is given as follows.

i) For a point $x: \text{Spec } \mathbb{F}_{q'} \rightarrow S$, consider the induced homomorphism

$$\pi_1^{\text{ét}}(x): \widehat{\mathbb{Z}} = \pi_1^{\text{ét}}(\text{Spec } \mathbb{F}_{q'}) \longrightarrow \pi_1^{\text{ét}}(S) \twoheadrightarrow \pi_1^t(S) \twoheadrightarrow \pi_1^t(S)^{\text{ab}}.$$

Send $[x]$ to $\pi_1^{\text{ét}}(x)(1)$. This defines a homomorphism $\iota'_S: h_0(S) \rightarrow \pi_1^t(S)^{\text{ab}}$.

ii) Clearly, the degree map $\deg: h_0(S) \rightarrow \mathbb{Z}$ is compatible with the homomorphism $\pi_1^t(S)^{\text{ab}} \rightarrow \pi_1^{\text{ét}}(\text{Spec } \mathbb{F}_q) = \widehat{\mathbb{Z}}$ induced by the structural morphism.

iii) The homomorphism ι_S is exactly the restriction of ι'_S to $\ker \deg$.

b) The map ι'_S defines an isomorphism $\widehat{h_0(S)} \rightarrow \pi_1^t(S)^{\text{ab}}$.

5.3 The tame fundamental group and the Picard group

5.3.1. Fact. — *Let V be a cubic ruled surface defined over the finite field \mathbb{F}_q . Then, $\pi_1^{t,\text{geo}}(V^{\text{reg}}) = 0$.*

Proof. It will suffice to show $\pi_1^t(V_{\mathbb{F}_q}^{\text{reg}}) = 0$. In the present situation, a smooth compactification of $V_{\mathbb{F}_q}^{\text{reg}}$ is given by a projective plane, blown up in one point. The preimage of the singular locus is a (double) line through the point blown up. Consequently, $V_{\mathbb{F}_q}^{\text{reg}}$ is a ruled surface over \mathbf{A}^1 . This yields $\pi_1^t(V_{\mathbb{F}_q}^{\text{reg}}) = 0$. □

5.3.2. Proposition. — *Let V be a geometrically irreducible cubic surface over \mathbb{F}_q that is not a cone. Suppose V is normal, i.e., of one of the types I.i). Then,*

$$\pi_1^{t,\text{geo}}(V^{\text{reg}})^{\text{ab}} = [(\text{Pic}(V^{\text{reg}})_{\text{prime to } p} \otimes_{\mathbb{Z}} \mu_{\infty}^{\vee})^{\text{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)}]^{\vee}.$$

Here, $^{\vee}$ denotes the Pontryagin dual, given by the functor $\text{Hom}(\cdot, \mathbb{Q}/\mathbb{Z})$.

Proof. *First step.* p -torsion.

We know a smooth compactification \overline{V} of V^{reg} , explicitly. $\overline{V}_{\mathbb{F}_q}$ is isomorphic to \mathbf{P}^2 blown-up in six points. In particular, we have $\pi_1^{\text{ét}}(\overline{V}_{\mathbb{F}_q}) = 0$. This suffices for $\pi_1^t(V_{\mathbb{F}_q})^{\text{ab}}_{p\text{-power}} = 0$ and $\pi_1^{t,\text{geo}}(V)_{p\text{-power}}^{\text{ab}} = 0$.

Second step. The Pontryagin dual.

Let us compute the Pontryagin dual $(\pi_1^{t,\text{geo}}(V^{\text{reg}})^{\text{ab}})^{\vee}$. For l prime to p , we have

$$\begin{aligned} \text{Hom}(\pi_1^{t,\text{geo}}(V^{\text{reg}})^{\text{ab}}, \tfrac{1}{l}\mathbb{Z}/\mathbb{Z}) &= \text{Hom}(\pi_1^t(V^{\text{reg}})^{\text{ab}}, \tfrac{1}{l}\mathbb{Z}/\mathbb{Z}) / \text{Hom}(\pi_1(\text{Spec } \mathbb{F}_q), \tfrac{1}{l}\mathbb{Z}/\mathbb{Z}) \\ &= \text{Hom}(\pi_1(V^{\text{reg}})^{\text{ab}}, \tfrac{1}{l}\mathbb{Z}/\mathbb{Z}) / \text{Hom}(\pi_1(\text{Spec } \mathbb{F}_q), \tfrac{1}{l}\mathbb{Z}/\mathbb{Z}) \\ &= H_{\text{ét}}^1(V^{\text{reg}}, \tfrac{1}{l}\mathbb{Z}/\mathbb{Z}) / H^1(\text{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q), \tfrac{1}{l}\mathbb{Z}/\mathbb{Z}). \end{aligned}$$

According to the Hochschild-Serre spectral sequence

$$H^p(\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q), H_{\mathrm{\acute{e}t}}^q(V_{\overline{\mathbb{F}}_q}^{\mathrm{reg}}, \tfrac{1}{l}\mathbb{Z}/\mathbb{Z})) \implies H_{\mathrm{\acute{e}t}}^{p+q}(V_{\overline{\mathbb{F}}_q}^{\mathrm{reg}}, \tfrac{1}{l}\mathbb{Z}/\mathbb{Z}),$$

the latter quotient is nothing but $H_{\mathrm{\acute{e}t}}^1(V_{\overline{\mathbb{F}}_q}^{\mathrm{reg}}, \tfrac{1}{l}\mathbb{Z}/\mathbb{Z})^{\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)}$.

Third step. The torsion part of the Picard group.

We have $\Gamma(V_{\overline{\mathbb{F}}_q}^{\mathrm{reg}}, \mathbb{G}_m) = \overline{\mathbb{F}}_q^*$. In fact, the A -, D -, and E -configurations do not contain any principal divisor. This immediately yields $H_{\mathrm{\acute{e}t}}^1(V_{\overline{\mathbb{F}}_q}^{\mathrm{reg}}, \mu_l) = \mathrm{Pic}(V_{\overline{\mathbb{F}}_q}^{\mathrm{reg}})_l$ for any l prime to p . On $V_{\overline{\mathbb{F}}_q}^{\mathrm{reg}}$, the sheaves μ_l and $\tfrac{1}{l}\mathbb{Z}/\mathbb{Z}$ coincide up to the Galois operation. We therefore have

$$\begin{aligned} \mathrm{Hom}(\pi_1^{t,\mathrm{geo}}(V^{\mathrm{reg}})^{\mathrm{ab}}, \tfrac{1}{l}\mathbb{Z}/\mathbb{Z}) &= (H_{\mathrm{\acute{e}t}}^1(V_{\overline{\mathbb{F}}_q}^{\mathrm{reg}}, \mu_l) \otimes_{\mathbb{Z}} \mu_l^{\vee})^{\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)} \\ &= (\mathrm{Pic}(V_{\overline{\mathbb{F}}_q}^{\mathrm{reg}})_l \otimes_{\mathbb{Z}} \mu_l^{\vee})^{\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)}. \end{aligned}$$

Summing this up over all l , we see that

$$(\pi_1^{t,\mathrm{geo}}(V^{\mathrm{reg}})^{\mathrm{ab}})^{\vee} = (\mathrm{Pic}(V^{\mathrm{reg}})_{\mathrm{prime\ to\ } p} \otimes_{\mathbb{Z}} \mu_{\infty}^{\vee})^{\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)},$$

which is equivalent to the assertion. \square

5.3.3. Summary. — Thus, in order to compute $A_0(V^{\mathrm{reg}})$, we only need to know $\mathrm{Pic}(V^{\mathrm{reg}})_{\mathrm{tors}}$ for each of the 21 types of cubic surfaces summarized in I.i).

5.4 The 21 types of normal cubic surfaces not being cones

5.4.1. Fact. — Let V be a normal, proper surface over an algebraically closed field and \tilde{V} its desingularization. Then,

$$\mathrm{Pic}(V^{\mathrm{reg}}) = \mathrm{Pic}(\tilde{V}) / \langle E_1, \dots, E_k \rangle,$$

where E_1, \dots, E_k denote the irreducible components of the preimages of the singularities on \tilde{V} . \square

5.4.2. Theorem. — Let V be an irreducible cubic surface over $\overline{\mathbb{F}}_q$, not being a cone. Suppose that V is normal, i.e., of one of the 21 types I.i).

Then, the Picard group $\mathrm{Pic}(V^{\mathrm{reg}})$ is torsion-free for 17 of the 21 types. For the four remaining types, the torsion is given in the table below.

type	singularities	$\mathrm{Pic}(V^{\mathrm{reg}})_{\mathrm{tors}}$
XVI	$4A_1$	$\mathbb{Z}/2\mathbb{Z}$
XVIII	$A_3 + 2A_1$	$\mathbb{Z}/2\mathbb{Z}$
XIX	$A_5 + A_1$	$\mathbb{Z}/2\mathbb{Z}$
XXI	$3A_2$	$\mathbb{Z}/3\mathbb{Z}$

Proof. We distinguish the cases systematically. Each time, we apply Fact 5.4.1. One has $\text{Pic}(\tilde{V}) \cong \mathbb{Z}^7$. The signature is $(1, -1, -1, -1, -1, -1, -1)$. I.e., we have torsion-freeness in the case of a smooth cubic surface.

Otherwise, the A -, D -, or E -configuration of (-2) -curves generates a sublattice of $\text{Pic}(\tilde{V})$. The quotient has torsion if and only if this sublattice can be refined in \mathbb{Z}^7 without enlarging the rank. This immediately shows torsion-freeness in the cases A_n for $n \neq 3$ and E_6 as the lattice discriminants are square-free.

For the other cases, the constructions described in [Do, page 278] yield explicit generators for sublattices of \mathbb{Z}^7 . We summarize them in the following table.

$2A_1$	$(2, -1, -1, -1, -1, -1, -1)$ $(0, 0, 0, 0, 0, 1, -1)$
A_3	$(0, 0, 0, 0, 0, 1, -1)$ $(0, 0, 0, 0, 1, -1, 0)$ $(0, 0, 0, 1, -1, 0, 0)$
$A_2 + A_1$	$A_1: (2, -1, -1, -1, -1, -1, -1)$ $A_2: (0, 0, 0, 0, 0, 1, -1)$ $A_2: (0, 0, 0, 0, 1, -1, 0)$
$3A_1$	$(2, -1, -1, -1, -1, -1, -1)$ $(0, 0, 0, 0, 0, 1, -1)$ $(0, 0, 0, 1, -1, 0, 0)$
$2A_2$	$1. A_2: (0, 0, 0, 0, 0, 1, -1)$ $1. A_2: (0, 0, 0, 0, 1, -1, 0)$ $2. A_2: (0, 0, 1, -1, 0, 0, 0)$ $2. A_2: (0, 1, -1, 0, 0, 0, 0)$
$A_3 + A_1$	$A_1: (2, -1, -1, -1, -1, -1, -1)$ $A_3: (0, 0, 0, 0, 0, 1, -1)$ $A_3: (0, 0, 0, 0, 1, -1, 0)$ $A_3: (0, 0, 0, 1, -1, 0, 0)$
D_4	$(1, -1, -1, -1, 0, 0, 0)$ $(0, 1, 0, 0, -1, 0, 0)$ $(0, 0, 1, 0, 0, -1, 0)$ $(0, 0, 0, 1, 0, 0, -1)$
$A_2 + 2A_1$	$1. A_1: (2, -1, -1, -1, -1, -1, -1)$ $2. A_1: (0, 0, 0, 0, 0, 1, -1)$ $A_2: (0, 0, 0, 1, -1, 0, 0)$ $A_2: (0, 0, 1, -1, 0, 0, 0)$
$A_4 + A_1$	$A_1: (2, -1, -1, -1, -1, -1, -1)$ $A_4: (0, 0, 0, 0, 0, 1, -1)$ $A_4: (0, 0, 0, 0, 1, -1, 0)$ $A_4: (0, 0, 0, 1, -1, 0, 0)$ $A_4: (0, 0, 1, -1, 0, 0, 0)$
D_5	$(1, -1, -1, 0, 0, 0, -1)$ $(0, 1, -1, 0, 0, 0, 0)$ $(0, 0, 1, -1, 0, 0, 0)$ $(0, 0, 0, 1, -1, 0, 0)$ $(0, 0, 0, 0, 1, -1, 0)$
$4A_1$	$(2, -1, -1, -1, -1, -1, -1)$ $(0, 0, 0, 0, 0, 1, -1)$ $(0, 0, 0, 1, -1, 0, 0)$ $(0, 1, -1, 0, 0, 0, 0)$
$2A_2 + A_1$	$A_1: (2, -1, -1, -1, -1, -1, -1)$ $1. A_2: (0, 0, 0, 0, 0, 1, -1)$ $1. A_2: (0, 0, 0, 0, 1, -1, 0)$ $2. A_2: (0, 0, 1, -1, 0, 0, 0)$ $2. A_2: (0, 1, -1, 0, 0, 0, 0)$

$A_3 + 2A_1$	1. $A_1: (2, -1, -1, -1, -1, -1, -1)$ 2. $A_1: (0, 0, 0, 0, 0, 1, -1)$ $A_3: (0, 0, 0, 1, -1, 0, 0)$ $A_3: (0, 0, 1, -1, 0, 0, 0)$ $A_3: (0, 1, -1, 0, 0, 0, 0)$
$A_5 + A_1$	$A_1: (2, -1, -1, -1, -1, -1, -1)$ $A_5: (0, 0, 0, 0, 0, 1, -1)$ $A_5: (0, 0, 0, 0, 1, -1, 0)$ $A_5: (0, 0, 0, 1, -1, 0, 0)$ $A_5: (0, 0, 1, -1, 0, 0, 0)$ $A_5: (0, 1, -1, 0, 0, 0, 0)$
$3A_2$	1. $A_2: (1, -1, -1, -1, 0, 0, 0) =: v_1$ 1. $A_2: (1, 0, 0, 0, -1, -1, -1) =: v_2$ 2. $A_2: (0, 1, -1, 0, 0, 0, 0) =: v_3$ 2. $A_2: (0, 0, 1, -1, 0, 0, 0) =: v_4$ 3. $A_2: (0, 0, 0, 0, 1, -1, 0) =: v_5$ 3. $A_2: (0, 0, 0, 0, 0, 1, -1) =: v_6$

Table 1: Sublattices in \mathbb{Z}^7 generated by the A -, D -, and E -configurations

The assertions now follow from mechanical calculations.

In the cases where torsion-freeness is claimed, one may easily extend the basis of the sublattice given to a basis of \mathbb{Z}^7 . For example, consider the types $A_n + A_1$. Then, we have subsets of the lattice base consisting of $2e_1 - e_2 - \dots - e_7$, $e_i - e_{i+1}$ for $i = 3, \dots, 6$, e_1 , and e_7 .

In the cases $4A_1$, $A_3 + 2A_1$, and $A_5 + A_1$, the lattices may indeed be extended by the vector $(1, 0, -1, 0, -1, 0, -1)$ without changing the ranks. The lattices obtained in this way are not further refinable within \mathbb{Z}^7 .

In the case $3A_2$, the vector $(v_1 + v_3 - v_4) - (v_2 + v_5 - v_6) = -3e_3 + 3e_6$ is obviously 3-divisible. The refined lattice has discriminant 3 and is, therefore, not refinable any further. \square

6 Surjectivity

6.1. Corollary. — *Let V be a geometrically irreducible cubic surface over \mathbb{F}_q , not being a cone. If*

$$\pi_V: \text{MW}(V) \longrightarrow A_0(V^{\text{reg}})$$

is not surjective then V^{reg} has a nontrivial finite covering which is trivial over every \mathbb{F}_q -rational point.

Proof. Under the assumption, the image of the canonical map $V^{\text{reg}}(\mathbb{F}_q) \rightarrow h_0(V^{\text{reg}})$ generates a subgroup which is not dense. Hence, there are $l > 1$ and a surjective, continuous homomorphism $\alpha: h_0(V^{\text{reg}}) \rightarrow \mathbb{Z}/l\mathbb{Z}$ sending the whole image of $V^{\text{reg}}(\mathbb{F}_q)$ to zero.

The same is true for the composition $\alpha \circ \iota'_{V^{\text{reg}}}: \pi_1^t(V^{\text{reg}}) \rightarrow \mathbb{Z}/l\mathbb{Z}$. But this simply means that the l -sheeted covering of V^{reg} defined by $\alpha \circ \iota'_{V^{\text{reg}}}$ has exactly l \mathbb{F}_q -rational points above every $x \in V^{\text{reg}}(\mathbb{F}_q)$. \square

6.2. Remark. — Suppose, π_V were not surjective. Then, according to the lemma, we have a nontrivial covering W such that $\#W(\mathbb{F}_q) = l\#V^{\text{reg}}(\mathbb{F}_q)$. The Weil conjectures, proven by P. Deligne, assure that this may be possible only for very small q .

6.3. Example. — Let V be a cubic surface of type $4A_1$ over the finite field \mathbb{F}_q . Then, the canonical homomorphism

$$\pi_V: \text{MW}(V) \longrightarrow A_0(V^{\text{reg}})$$

is surjective for $q > 13$.

Proof. Assume the contrary. Then, according to Corollary 6.1, we have a twofold covering $p: V' \rightarrow V$ ramified at the four singularities such that, over every smooth \mathbb{F}_q -rational point of V , there are two of V' . Being a cubic surface, V has at least $q^2 - 5q + 1$ points. Hence, $\#V^{\text{reg}}(\mathbb{F}_q) \geq q^2 - 5q - 3$.

On the other hand, $\chi_{\text{top}}(V) = 3 + 6 - 4 \cdot 2 = 1$, as V^{reg} is \mathbf{P}^2 blown up in six points with four lines deleted. Therefore, $\chi_{\text{top}}(V') = 6$. Indeed, V' consists of the two sheets above V^{reg} and four points of ramification.

We claim $\#V'(\mathbb{F}_q) \leq q^2 + 4q + 1$. For this, first observe that V' is simply connected as, otherwise, V^{reg} had more coverings than the twofold one. Let k be the number of blow-ups necessary in order to desingularize V' . Then, $\dim H_{\text{ét}}^2(\overline{V}, \mathbb{Q}_l) = k + 4$ and one has the naive estimate $\#\overline{V}(\mathbb{F}_q) \leq q^2 + (k + 4)q + 1$. The claim follows.

Consequently, $2(q^2 - 5q - 3) \leq 2\#V^{\text{reg}}(\mathbb{F}_q) \leq \#(V')^{\text{reg}}(\mathbb{F}_q) \leq q^2 + 4q + 1$, which implies $q \leq 14$, immediately. \square

7 Some observations

7.1. Lemma. — *Let V be a cubic surface over the finite field \mathbb{F}_q . Suppose that, in every equivalence class of $V^{\text{reg}}(\mathbb{F}_q)$, there is a point not contained in any of the lines lying on V .*

i) *Suppose $\#\text{MW}(V) = 2$. Assume further that not all points of $V^{\text{reg}}(\mathbb{F}_q)$ are contained in a plane. Then, for the two equivalence classes M_0, M_1 of $V^{\text{reg}}(\mathbb{F}_q)$, we have the relation $\#M_1 - \#M_2 = \pm q$.*

ii) *Suppose $\#\text{MW}(V) = 3$. Then, the three equivalence classes M_0, M_1, M_2 of $V^{\text{reg}}(\mathbb{F}_q)$ are of the same size.*

Proof. i) Without restriction, assume that the classes are denoted in such a way that a line not entirely contained in V always meets zero or two points from M_1 .

Then, fix a point $x \in M_1$ not contained in a line lying on V . By assumption, there is some $x' \in V^{\text{reg}}(\mathbb{F}_q)$ outside the plane tangent at x . The line g connecting x and x' meets V in two distinct points $x, y \in M_1$ and in $z \in M_0$.

Now, we intersect V with the pencil of planes containing g . We assert that each of the curves C_t arising contains as many points from M_0 as from M_1 . This immediately implies the assertion. Indeed, equinumerosity occurs as soon as we count the points x , y , and z multiply.

Let now C_t be one of the intersection curves. We first observe that $x \in C_t$ is a smooth point. In fact, we do not intersect V with the tangent plane at x since that does not contain g . C_t may be reducible. However, x is, by assumption, not contained in a line. Therefore, for every $p \in C_t(\mathbb{F}_q)$, there is a unique $p' \in C_t(\mathbb{F}_q)$ such that x , p , and p' are collinear. As p and p' are in different classes, the assertion follows.

ii) Here, there are two cases.

First case. If $x \in M_i$, $y \in M_j$, and $z \in M_k$ are the three points of intersection of a line with V then $i + j + k \equiv 0 \pmod{3}$.

We choose a point $x \in M_0$ which is not contained in any of the lines on V . Then, for every $p \in M_1$, there is a unique $p' \in M_2$ such that x , p , and p' are collinear. As this assignment is invertible, one has $\#M_1 = \#M_2$. Analogously, a starting point $x \in M_1$ yields the equality $\#M_2 = \#M_0$.

Second case. If $x \in M_i$, $y \in M_j$, and $z \in M_k$ are the three points of intersection of a line with V then $i + j + k \not\equiv 0 \pmod{3}$.

We may assume without restriction that $i + j + k \equiv 1 \pmod{3}$. Choose a point $x \in M_0$ which is not contained in any of the lines on V . The tangent plane T_x contains, besides x , only points from M_1 . Further, there are exactly $q + 1$ of them, as, by the assumption of this case, there is no line tangent at x of order three. On the other hand, outside T_x , the sets M_0 and M_1 are equinumerous since the lines through x cause a bijection. Consequently, $\#M_1 = \#M_0 + q$.

Analogously, we obtain $\#M_2 = \#M_1 + q$ and $\#M_0 = \#M_2 + q$ when starting with a point $x \in M_1$ or $x \in M_2$, respectively. Thus, the second case is contradictory. \square

7.2. Definition. — Let V be a cubic surface over the finite field \mathbb{F}_q such that $\#\text{MW}(V) = 2$. Then, $V^{\text{reg}}(\mathbb{F}_q)$ decomposes into exactly two equivalence classes. We will call the equivalence class *negative* that occurs an even number of times on each line.

7.3. Lemma (Connection to the Hessian). —

Let V , given by $F(X_0, \dots, X_3) = 0$, be a cubic surface over the finite field \mathbb{F}_q of characteristic $\neq 2$. Suppose $\#\text{MW}(V) = 2$. Then, the following is true.

If $p \in V^{\text{reg}}(\mathbb{F}_q)$ is a negative point not lying on a line contained in V then the Hessian

$$\det \frac{\partial^2 F}{\partial X_i \partial X_j}(p)$$

is a non-square in \mathbb{F}_q .

Proof. Consider the tangent plane T_p at p . The intersection $C_p := V \cap T_p$ is a cubic curve with a singularity at p . Thus, in affine coordinates and locally near p , the equation of C_p is of the form $Q(x, y) + K(x, y) = 0$ for a quadratic form Q and a cubic form K .

By assumption, there is no line in T_p meeting p with multiplicity 3. This means, in particular, that $p \in C_p$ is a double point, not a triple point. Further, the two tangent directions at p are not defined over \mathbb{F}_q . In other words, the binary quadratic form Q does not represent zero over \mathbb{F}_q . This exactly means that minus the discriminant of Q is a non-square in \mathbb{F}_q . It is a direct calculation to show that $(-\text{disc } Q)$ coincides, up to square factors, with the Hessian of F at p . \square

8 Experiments

8.1. Description of the sample. — We let p run through the prime numbers from 5 through 101. For each of the primes, we followed the classification of cubic surfaces as described in 2.2 and 2.3. For each type, we selected ten examples by help of a random number generator. For those types which clearly have no moduli, we took only one example. We avoided the surfaces decomposing into three planes over a proper extension of \mathbb{F}_p as, for these, $\text{MW}(V)$ is known to degenerate. All in all, we worked with 330 cubic surfaces per prime.

For each surface, we determined the partition of $V(\mathbb{F}_p)$ into equivalence classes. For this, we run an implementation of Algorithm A.3 in `magma`.

8.2. The results. — The partition of the points found allowed us to determine $\text{MW}(V)$ for every surface in the sample.

There is another observation, which is by far more astonishing. In each case, according to the theory described, we know an abelian group, $\text{MW}(V)$ naturally surjects to. It turned out that $\text{MW}(V)$ was equal that group with only one exception.

The exception occurred for $p = 5$. It was the cone over the elliptic curve given by $y^2 = x^3 + 2x$. As this elliptic curve has only two \mathbb{F}_5 -rational points, the construction of $\text{MW}(V)$ must degenerate.

8.3. Remark. — This effect clearly becomes much worse for $p = 2$ or 3. This is one of the reasons why these primes were excluded from the experiments.

8.4. Summary. — *Case I.i)* Among the normal cubic surfaces having only double points, we always found $\text{MW}(V) = 0$ except for the cases $4A_1$, $A_3 + 2A_1$, $A_5 + A_1$, and $3A_2$. In the first three of these cases, we have $\text{MW}(V) = \mathbb{Z}/2\mathbb{Z}$.

Finally, in the case $3A_2$, we established that $\text{MW}(V) = \mathbb{Z}/3\mathbb{Z}$ for $p \equiv 1 \pmod{3}$ and Frobenius acting on the singular points by an even permutation and for $p \equiv 2 \pmod{3}$ and Frobenius acting by an odd permutation. Otherwise, $\text{MW}(V) = 0$.

Cases I.ii) and II.ii) Ignoring the exception mentioned, for the cones, $\text{MW}(V)$ was always equal to the Mordell-Weil group of the underlying curve.

Case II.i) The cubic ruled surfaces always fulfilled $\text{MW}(V) = 0$.

Two components. When V consisted of a non-degenerate quadric and a plane, we always found that $\text{MW}(V) = \mathbb{Z}$, two points being equivalent if and only if they belonged to the same component. When the quadric was a cone and the plane did not meet the cusp, it turned out that $\text{MW}(V) = \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, the surjection described in Example 4.2 being bijective.

A cubic surface consisting of a cone and a plane through the cusp is a cone over a reducible cubic curve. Here, $\text{MW}(V)$ was always isomorphic to the Mordell-Weil group of the curve.

Three components. A cubic surface consisting of three planes meeting in a point is the cone over a triangle. $\text{MW}(V)$ was always equal to the Mordell-Weil group of the triangle.

Finally, three planes meeting in a line form a cone in many ways. Hence, two distinct points are never equivalent to each other. We have $\text{MW}(V) \cong (K^+)^2 \oplus \mathbb{Z}^2$.

8.5. Remark. — The case of a cubic surface consisting of three planes with a line in common is the easiest from the theoretical point of view. For Algorithm A.3, it is, however, the most complicated one. No simplification occurs as no equivalent points may be found. The running time is dominated by steps iv) and v), which are otherwise negligible. For $p > 70$, we excluded this case from the experiments.

8.6. Remark. — On a Quad-Core AMD Opteron Processor 2356, the total CPU time was eight minutes for $p = 5$, a little less than an hour for $p = 37$, three and a half hours for $p = 71$, and more than ten hours for $p = 101$.

A Algorithms

A.1. Algorithm (Equivalent points). — i) Using a random number generator, choose four distinct points $x_{11}, x_{12}, x_{21}, x_{22} \in V^{\text{reg}}(\mathbb{F}_q)$.

ii) Determine four points $x_{13}, x_{23}, x_{31}, x_{32} \in V^{\text{reg}}(\mathbb{F}_q)$ such that the relations $[x_{11}, x_{12}, x_{13}]$, $[x_{21}, x_{22}, x_{23}]$, $[x_{11}, x_{21}, x_{31}]$, and $[x_{12}, x_{22}, x_{32}]$ are fulfilled. If this turns out to be impossible as (x_{11}, x_{12}) , (x_{21}, x_{22}) , (x_{11}, x_{21}) , or (x_{12}, x_{22}) are lying on a line completely contained in V then output FAIL and terminate prematurely.

iii) Determine points x_{33} and x'_{33} such that $[x_{13}, x_{23}, x_{33}]$ and $[x_{31}, x_{32}, x'_{33}]$. If this turns out to be impossible as (x_{13}, x_{23}) or (x_{31}, x_{32}) are lying on a line completely contained in V then output FAIL and terminate prematurely.

iv) Output “ x_{33} and x'_{33} are equivalent.”

A.2. Algorithm (A point being equivalent to a given $x_0 \in V^{\text{reg}}(\mathbb{F}_q)$). —

- i) Execute Algorithm A.1 in order to find two mutually equivalent points x_1 and x_2 .
- ii) Determine a point x'_1 such that $[x_1, x_0, x'_1]$. If this turns out to be impossible as (x_1, x_0) are lying on a line completely contained in V then output FAIL and terminate prematurely.
- iii) Now, determine a point x'_0 such that $[x'_1, x_2, x'_0]$. If this turns out to be impossible as (x'_1, x_2) are lying on a line completely contained in V then output FAIL and terminate prematurely.
- iv) Output “ x'_0 is equivalent to x_0 .”

A.3. Algorithm (Partition of the points). —

- i) Choose a natural number N .
- ii) Decompose $V^{\text{reg}}(\mathbb{F}_q)$ into a set $\mathfrak{M} = \{N_1, \dots, N_m\} = \{\{x_1\}, \dots, \{x_m\}\}$ of singletons.
- iii) Execute Algorithm A.1, Nq^2 times. When two equivalent points $x_1 \in M_k$ and $x_2 \in M_l$ for $k \neq l$ are found, unite M_k with M_l and reduce m by 1.
- iv) List the singletons still contained in \mathfrak{M} , i.e., the points that were never met in step iii). For each element in the list obtained, execute Algorithm A.2 N times. When two equivalent points $x_1 \in M_k$ and $x_2 \in M_l$ for $k \neq l$ are found, unite M_k with M_l and reduce m by 1.
- v) If sets of size less than q remain in \mathfrak{M} then choose a single element from each of these sets. For each element in the list obtained, execute Algorithm A.2 N times. When two equivalent points $x_1 \in M_k$ and $x_2 \in M_l$ for $k \neq l$ are found, unite M_k with M_l and reduce m by 1.
- vi) Output the partition of $V^{\text{reg}}(\mathbb{F}_q)$ found.

A.4. Remarks. — i) Algorithm A.3 finds a partition which is possibly too fine in comparison with the actual partition into equivalence classes.

ii) In practice, the value $N = 7$ seems to work perfectly, for $p = 5$ as well as for the biggest primes for which such an algorithm seems reasonable.

References

- [B] Bright, M. J.: *Efficient evaluation of the Brauer-Manin obstruction*, Math. Proc. Cambridge Philos. Soc. **142** (2007), 13–23
- [Do] Dolgachev, I. V.: Topics in classical algebraic geometry, Part I, available at: <http://www.math.lsa.umich.edu/~idolga/topics1.pdf>

- [EJ] Elsenhans, A.-S. and Jahnel, J.: *On the Brauer–Manin obstruction for cubic surfaces*, to appear in: *Journal of Combinatorics and Number Theory*
- [Li] Lichtenbaum, S.: *Duality theorems for curves over p -adic fields*, *Invent. Math.* **7** (1969), 120–136
- [Ma] Manin, Yu. I.: *Cubic forms, algebra, geometry, arithmetic*, North-Holland Publishing Co. and American Elsevier Publishing Co., Amsterdam, London, and New York 1974
- [Sch] Schmidt, A.: Singular homology of arithmetic schemes, *Algebra & Number Theory* **1** (2007), 183–222
- [SchS] Schmidt, A. and Spieß, M.: Singular homology and class field theory of varieties over finite fields, *J. Reine Angew. Math.* **527** (2000), 13–36
- [SGA1] Grothendieck, A.: *Revêtements étales et groupe fondamental*, Lecture Notes in Math. 224, *Springer*, Berlin 1971
- [SV] Suslin, A. and Voevodsky, V.: Singular homology of abstract algebraic varieties, *Invent. Math.* **123** (1996), 61–94